

# 基于分块的小波域图像半脆弱水印认证算法

武凤翔<sup>1</sup>, 岳晓丽<sup>2</sup>, 徐江峰<sup>2</sup>

(1. 华北水利水电学院 水利职业学院, 河南 郑州 450002; 2. 郑州大学 信息工程学院, 河南 郑州 450001)

**摘 要:** 提出一种图像半脆弱水印认证算法, 该算法将图像分成四块, 从三级小波分解的低频系数中提取每部分图像的特征作为水印, 嵌入到载体图像的各分块中, 水印提取既不需要原始图像, 也不需要原始水印信息. 理论分析及实验结果表明, 该算法可以对任意大小的载体图像进行水印嵌入, 具有很好的透明性, 不仅能抵御噪声、有损压缩等非恶意攻击, 还能有效地检测定位剪切、替换等恶意攻击.

**关键词:** 半脆弱水印; 分块; 小波变换; 图像认证

**中图分类号:** TN911.73; TP309.7 **文献标志码:** A **doi:**10.3969/j.issn.1671-6833.2012.02.003

## 0 引言

在数字水印系统中, 有两种技术被广泛的研究, 即鲁棒性水印和脆弱性水印. 鲁棒水印主要是为了版权保护, 用以抵御各种试图移去或毁坏水印的攻击, 但它不能判定图像内容是否被篡改; 而脆弱水印则可以识别对水印嵌入图像的任何篡改, 但鲁棒性较差, 不能忍受对图像的任何处理, 即使是常用的 JPEG 压缩、直方图均匀化等操作. 半脆弱水印则集合了二者的优点, 既可容忍对图像一定程度的信号处理, 也可以检测、定位对图像的篡改<sup>[1-2]</sup>.

目前的水印算法, 几乎都是针对大小为  $2^L \times 2^L$  的标准载体图像展开的, 其中  $L$  表示小波变换的级数. 而在实际使用过程中用到的图像规格则多种多样, 现有的水印算法无法处理. 同时由于 JPEG 压缩应用的普遍性, 在保持较高的篡改检测能力情况下, 提高抗 JPEG 压缩性能也是半脆弱水印研究的重要问题. 为此, 笔者提出了一种新的半脆弱水印认证算法, 该算法通过对图像的分块处理, 实现了对任意大小载体图像的水印嵌入. 仿真实验表明, 该算法具有较好的篡改检测及定位能力, 可以有效提高系统抵抗 JPEG 压缩性能.

## 1 图像的小波分解

小波变换具有很好的多分辨率分析特性, 在

当前的水印算法中被广泛使用<sup>[3-4]</sup>. 图 1 给出了基于小波变换的静态图像的金字塔式多分辨率分解示意图. 对于三级小波分解后的图像数据而言, 高频子带就是  $D_k^0, D_k^1, D_k^2 (k=1, 2, 3)$  3 个频带序列, 它们分别表示图像中水平方向、对角方向和垂直方向的边缘、轮廓和纹理等. 低频子带则是  $A_3^3$  所代表的部分, 它集中了原始图像的绝大部分能量. 由小波变换的图像多分辨率分解特点可以看出, 它具有良好的空间方向选择性, 与人的视觉特性十分吻合. 低频子带具有较强的抵抗外来影响的能力, 稳定性较好; 而高频子带容易受外来噪声、图像处理操作等影响, 稳定性较差. 因此在低频子带中嵌入水印可以较好的满足鲁棒性; 而在高频子带中嵌入水印, 则可以较好的满足水印对攻击的脆弱性, 从而达到认证的目的<sup>[5-7]</sup>.

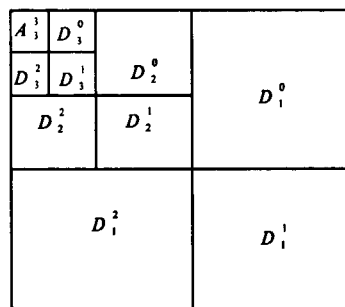


图 1 三级小波分解示意图

Fig. 1 Three level wavelet decomposition diagram

收稿日期:2011-10-28; 修订日期:2011-12-25

基金项目:国家自然科学基金资助项目(61071211)

作者简介:武凤翔(1962-), 男, 河南禹州人, 华北水利水电学院副教授, 主要从事数字水印方面的研究, E-mail: xxgex62@126.com.

## 2 基于分块的小波域图像半脆弱水印认证算法

认证水印系统主要包括以下步骤:首先将提取的宿主图像信息转变为水印信号嵌入原始图像中,而后嵌入水印的图像经过信道传输到接收端.最后接收者对待测图像进行检测认证.为了加强安全性,在嵌入和检测的过程中还需借助密钥<sup>[7]</sup>.

设计一个图像内容认证系统还应考虑以下问题:①检测的是内容的篡改而不是图像的不同表示;②附加的信息不应过大;③当有内容篡改时系统不仅要指出有篡改事件发生,同时也要指出内容更改的位置<sup>[8]</sup>.

笔者给出的算法载体图像可以是任何尺寸,进行处理时首先把图像分成四部分,之后按照处理标准图像的方法进行处理.假定载体图像尺寸为  $M \times N$ ,图像分割后的每部分尺寸记为  $m \times n$ ,则  $m = M - \text{mod}(M, 8) - K \times 2^L$ ,  $n = N - \text{mod}(N, 8) - K \times 2^L$ ,其中  $\text{mod}$  是取余函数,  $K$  是分割后图像的扩展比例因子,  $L$  是小波变换的级数.

### 2.1 水印嵌入算法

#### 2.1.1 水印的生成

(1) 图像划分. 首先要把载体图像分成大小相同的四部分: XLU 是原图像的左上部分, 由块 1, 2, 4, 5 组成; XRU 是原图像的右上部分, 由块 2, 3, 5, 6 组成; XLD 是原图像的左下部分, 由块 4, 5, 7, 8 组成; XRD 则是原图像的右下部分, 由块 5, 6, 8, 9 组成, 如图 2 所示.

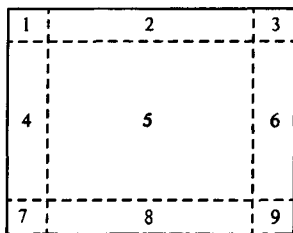


图2 分块示意图

Fig.2 Block diagram

(2) 生成基于图像内容的水印. 图像划分之后, 从三级小波分解的低频系数中提取每部分图像的特征作为嵌入水印. 为了提高安全性, 还可以对产生的水印先进行加密, 而后再进行嵌入.

#### 2.1.2 水印的嵌入

(1) 计算三级小波分解中二层高频水平和垂直方向的掩蔽阈值, 并分别记作  $T_l$  和  $T_h$ ;

(2) 生成水印信息  $e$ ;

(3) 二层水平和垂直方向系数分别记作  $V$  和

$H$ , 由于二层系数矩阵的大小为  $m/4 \times n/4$ , 水印  $e$  的大小为  $m/8 \times n/8$ , 所以需要将  $V$  和  $H$  按相邻四块为一大块进行划分, 以使水印序列的每个值对应一个块. 嵌入规则如下:

如果  $e(i/2, j/2) = 1$ ,

$$\begin{cases} V(i, j) = V(i, j) + |T_l(i/2, j/2)| + \\ 15 - F(i/2, j/2)/6; \\ H(i, j) = H(i, j) - |T_h(i/2, j/2)| + \\ 15 - F(i/2, j/2)/6; \end{cases}$$

否则,

$$\begin{cases} V(i, j) = V(i, j) - |T_l(i/2, j/2)| + \\ 15 + F(i/2, j/2)/6; \\ H(i, j) = H(i, j) + |T_h(i/2, j/2)| + \\ 15 + F(i/2, j/2)/6. \end{cases}$$

其中,  $1 \leq i \leq m/4$ ,  $1 \leq j \leq n/4$ ,  $F(i, j) = \sum_{p=2i-1}^{2i} \sum_{q=2j-1}^{2j} (V(p, q) - H(p, q))$ . 当嵌入的水印为 1 时,  $F(i, j) \geq 0$ ; 当嵌入的水印为 0 时,  $F(i, j) < 0$ .

使用该算法分别对 XLU、XLD、XRU、XRD 进行水印嵌入, 得到 4 组水印嵌入后的图像. 然后再按照类似原始图像分割的方法, 对 4 组嵌入图像进行整合得到和原始图像大小相同的水印嵌入图像. 整合时以 XLU 水印嵌入图像为主, 缺少的行和列分别使用 XLD、XRU、XRD 水印嵌入后的图像的行列来补齐. 最后对整合后的图像进行逆三级小波变换, 即可得到嵌入水印的图像. 水印嵌入流程如图 3 所示.

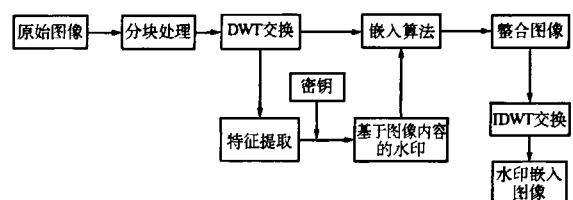


图3 水印嵌入流程

Fig.3 Watermarking embed process

### 2.2 水印提取和认证

#### 2.2.1 水印的提取

(1) 分块提取. 把接收方的图像记为  $X'$ , 划分得到的四部分分别记作  $X'LU$ 、 $X'LD$ 、 $X'RU$ 、 $X'RD$ . 水印提取的过程实际就是水印嵌入的逆过程, 而且整个提取过程既不需要原始图像也不需要原始水印信息. 与水印嵌入类似, 以  $X'LU$  为例描述提取过程, 其中

$$F'(i, j) = \sum_{p=2i-1}^{2i} \sum_{q=2j-1}^{2j} (V'(p, q) - H'(p, q)),$$

式中:  $V'$  和  $H'$  分别表示对  $X'LU$  进行三级小波分

解后二层的高频水平和垂直系数. 提取时, 如果  $F'(i,j) \geq 0$ , 则  $E(i,j) = 1$ ; 否则  $E(i,j) = 0$ ; 最后对  $E$  进行解密即可得到水印 ELU.

对另外三部分做同样的操作, 得到水印分别记为 ELD、ERU、ERD.

(2) 水印整合. 分别提取四块水印之后, 再对它们整合得到最终提取的水印, 整合参照水印嵌入后进行图像整合的比例, 具体如图 4 所示.

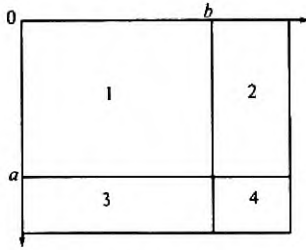


图 4 提取水印整合图示

Fig. 4 Extraction of watermarking integration diagram

整合时用到的一些变量, 定义如下:

$R_D = (M - 2 \times \text{mod}(M, 8) + 1 - 2 \times K \times 2^L) / m$ , 代表 XLD、XRD 截取行数的比例;

$R_U = (N - 2 \times \text{mod}(N, 8) + 1 - 2 \times K \times 2^L) / n$ , 代表 XRU 截取列数的比例;

$S_D = R_D \times a$ , 代表从水印 ELD、ERD 中截取数据的起始行号;

$S_U = R_U \times b$ , 代表从水印 ERU 中截取数据的起始列号;

$L_D = a - S_D + 1$ , 代表从水印 ELD、ERD 截取数据的行长度,  $a = m/8$ ;

$L_U = b - S_U + 1$ , 代表从水印 ERU 截取数据的列长度,  $b = n/8$ .

其中,  $R_D$  是图 2 中块 7 所占的行数在块 4 和块 7 所占总行数中的比例; 整合后的水印记为  $W$ , 具体整合方法如下:

$$W(1:a, 1:b) = \text{ELU};$$

$$W(a+1:a+L_D, 1:b) = \text{ELD}(S_D:a, 1:b);$$

$$W(1:a, b+1:b+L_U) = \text{ERU}(1:a, S_U:b);$$

$$W(a+1:a+L_D, b+1:b+L_U) = \text{ERD}(S_D:a, S_U:b).$$

### 2.2.2 认证

首先, 要按照嵌入时使用的方法, 分别对  $X'LU$ 、 $X'LD$ 、 $X'RU$ 、 $X'RD$  进行特征提取, 之后使用整合水印的方式, 对四部分特征进行整合得到最终的整体图像特征, 记作  $TZ$ , 最后用提取的水印  $W$  和重新生成的特征  $TZ$  进行比较, 得到篡改矩阵, 水印提取和篡改认证过程如图 5 所示.

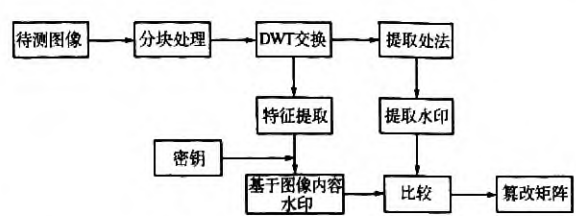
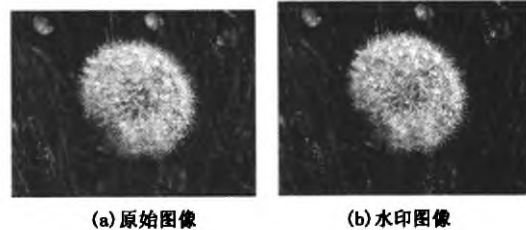


图 5 水印提取和篡改认证

Fig. 5 Watermarking extraction and image authentication

## 3 实验结果及分析

实验结果都是基于 MATLAB7.0 的仿真得到的, 实验图像采用  $599 \times 791$  的非标准灰度图像. 加密采用基于 logistic 混沌系统的加密算法, 生成安全的水印序列, 如图 6 所示. 从图 6 可以看出, 水印嵌入前后几乎没有引起视觉上的变化, 并且获得较高的峰值信噪比.



(a) 原始图像 (b) 水印图像

图 6 原始图像和半易损水印图像

Fig. 6 Original image and semi-fragile watermarking image

水印图像可能遭受两类典型的攻击: 一种是非恶意的, 如图像传送过程中的信道噪声、有损压缩等; 另一种是恶意的, 如图像剪切、替换等操作.

### 3.1 非恶意攻击测试

测试包括通用信号处理, 如噪声叠加、滤波、有损压缩等. 该系统能够检测到篡改区域, 篡改检测结果如图 7 所示.

从实验结果可以看出, 系统能够检测到篡改区域, 并能有效地抵御 JPEG 压缩攻击, 当压缩因子为 20 时, 检测到篡改区域仍然不是很多, 对有损压缩有较强的鲁棒性.

### 3.2 恶意攻击测试

恶意攻击主要包括图像剪切、替换操作. 图 8 给出了剪切攻击的实验结果, 图 9 给出了替换攻击的实验结果, 图 10 给出了一个复合攻击的实验结果.

从图 7, 8 可以看出: 该算法不但能够抵御非恶意的攻击, 如: 加入噪声、滤波、JPEG 压缩等, 还能对剪切、替换等恶意攻击进行有效的定位.

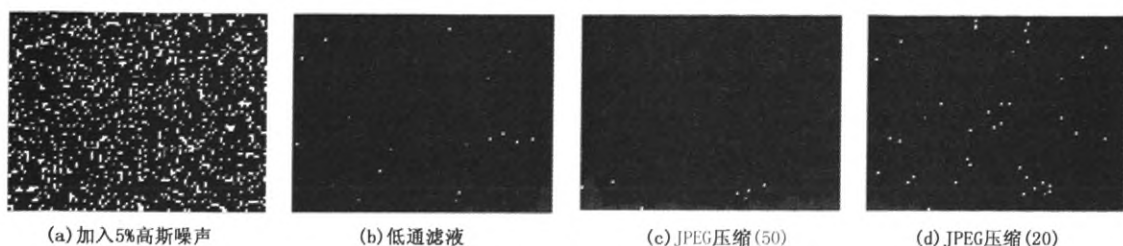


图7 非恶意攻击

Fig.7 The non-malicious attacks

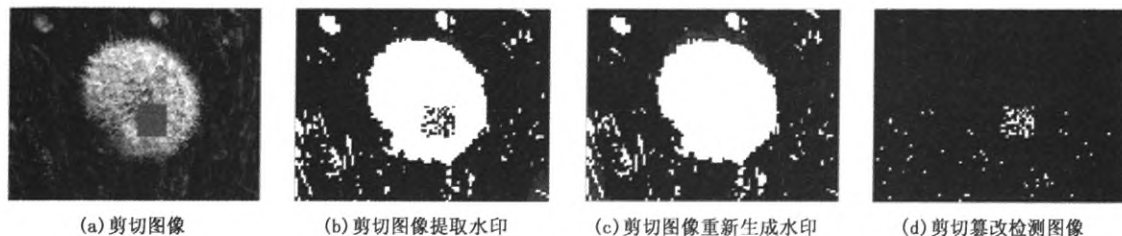


图8 剪切攻击实验结果

Fig.8 The detecting result of replacing image

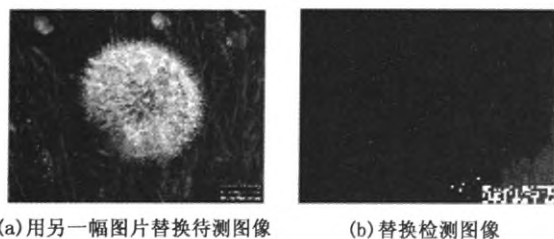


图9 替换攻击实验结果

Fig.9 The detecting result of cutting attack

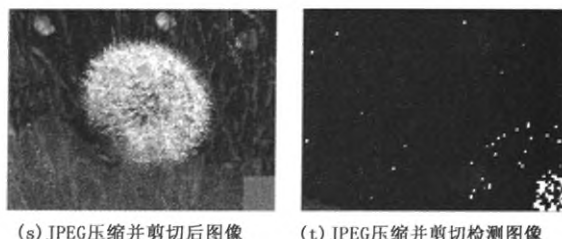


图10 JPEG压缩并剪切攻击实验结果

Fig.10 The detecting result of JPEG compress and cutting image

## 4 结论

提出了一种基于分块的小波域图像半脆弱水印认证算法,该算法通过对图像的划分,可以对任意大小图像进行水印嵌入,解决了传统算法只能对标准尺寸图像进行认证问题.该算法嵌入的水印信息是从载体图像中提取的,因而图像认证时,既不需要原始图像,也不需要原始的水印信息,接收者通过把接收图像提取出的水印信息与从接收图像产生的水印信息进行比较,即可实现图像的认证,在有篡改攻击时确定出篡改位置.

## 参考文献:

- [1] 李春,黄继武.一种抗JPEG压缩的半脆弱图像水印算法[J].软件学报,2006,17(2):313-324.
- [2] 易开祥,孙鑫,王道顺,等.一种新的基于图像内容的半易损水印技术[J].系统仿真学报,2002,9

(14):1200-1203.

- [3] QI Hui-yuan, ZHENG Dong, ZHAO Ji-ying. Human visual system based adaptive digital image watermarking [J]. Signal Processing, 2008, 88(1): 174-188.
- [4] LEWIS A S, KNOELES G. Image compression using the 2-D wavelet transform [J]. Image Processing, 1992, 2(1): 244-250.
- [5] BAMI M, BARTOLINI E, PIVA A. Improved wavelet-based watermarking through pixel-wise masking [J]. Image Processing, 2001, 5(10): 783-791.
- [6] 赵洋,孙燮华. HVS的DWT域半脆弱水印算法[J].中国计量学院学报,2008,19(4):333-337.
- [7] 侯振华,陈生潭.脆弱性数字水印研究[J].计算机应用,2003,23(12):106-108.
- [8] 沃森,韩国强,张坚威,等.基于小波变换和形态学的图像内容认证方法[J].通信学报,2005,26(8): 9-15.

(下转第18页)

- based fault detection for nonlinear networked systems with random packet dropout and time-varying delay [C]// Proc of the 29th Chinese Control Conference, Piscataway, NJ, United States; IEEE Computer Society, 2010: 4278 - 4282.
- [4] 李娟, 唐功友. 基于观测器的离散时滞系统的故障诊断[J]. 控制与决策, 2010, 25(8): 1220 - 1224.
- [5] 张端金, 王忠勇, 吴捷. 系统控制和信号处理中的 Delta 算子方法[J]. 控制与决策, 2003, 18(4): 385 - 391.
- [6] MIDDLETON R H, GOODWIN G C. Improved finite word length characteristics in digital control using delta operator [J]. IEEE Trans on Automatic Control, 1986, 31(11): 1015 - 1021.
- [7] MIDDLETON R H, GOODWIN G C. Digital Control and Estimation [M]. London: PrenticeHall Inc, 1990: 41 - 51.
- [8] 王红茹, 王常虹, 高会军. 时滞离散不确定系统的鲁棒故障检测[J]. 电机与控制学报, 2006, 10(5): 503 - 507.
- [9] 王红茹, 王常虹, 高会军. 时滞离散 LPV 系统的鲁棒故障检测与分离[J]. 哈尔滨工业大学学报, 2007, 39(9): 1352 - 1355.

### Fault Detection Filter for Delta Operator-Based Systems with Time-Delay

ZHANG Duan-jin, MENG Shan, GUO Hao, GUAN Li-li

(School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

**Abstract:** This paper studies the design problem of robust fault detection filters for Delta operator discrete systems with state delays. Based on the traditional filter using the shift operator, a new filter model to fault detection for Delta operator systems with time-delay is given. Sufficient conditions for the existence of the robust fault detection filter and its explicit expressions are developed in terms of linear matrix inequalities (LMIs) approach. When LMIs are feasible, the optimal robust fault detection filters of Delta operator formulated systems are obtained. The presented results can bring the fault detection for continuous time systems and discrete time systems into the unified Delta operator framework. The simulations show the effectiveness of the proposed approach.

**Key words:** discrete time systems with time-delay; fault detection; Delta operator; filter model

(上接第 13 页)

### A Semi-fragile Watermarking Authentication Algorithm Based on Block and Wavelet Domain of Image

WU Feng-xiang<sup>1</sup>, YUE Xiao-li<sup>2</sup>, XU Jiang-feng<sup>2</sup>

(1. Water Conservancy Vocational School, North China Institute of Water Conservancy and Hydroelectric Power, Zhengzhou 450002, China; 2. School of Information Engineering, Zhengzhou University, Zhengzhou 450001, China)

**Abstract:** A new semi-fragile watermarking authentication algorithm is proposed, the algorithm first divides the image into four blocks, then the feature of each block of image is extracted from low frequency coefficient of three level wavelet transform, and then the feature as the watermark is embedded into corresponding block of image, the four blocks embedded into watermark were combined into a new image. The watermark can be extracted without involving either the host image or the original watermark. Theoretical analysis and experimental results show that the algorithm can be carriers of images of any size, and with good transparency, and it can not only resist non-malicious attacks, such as noise and lossy compression, it can also effectively detect and locate the cut, replaced, and other malicious attacks.

**Key words:** semi-fragile watermark; block; wavelet transform; image authentication